Rekomendacje w związku ze zwiększonym zagrożeniem w cyberprzestrzeni wywołanym sytuacją na Ukrainie

Każdy z nas codziennie jest narażony na zagrożenia w cyberprzestrzeni, ale są momenty, gdy czujność trzeba jeszcze dodatkowo wzmocnić. W związku z obecną sytuacją na Ukrainie oraz ogłoszeniem stopnia alarmowego CHARLIE-CRP, przygotowaliśmy rekomendacje dla obywateli i firm, których wdrożenie uważamy za konieczne. Jeśli do tej pory Twoja firma nie testowała nigdy procedury przywracania kopii zapasowych, to jest to właściwy moment na zrobienie tego.

Rekomendacje dla obywateli

- Zapoznaj się z poradnikiem dotyczącym bezpieczeństwa skrzynek pocztowych i kont w mediach społecznościowych oraz zastosuj się do jego rekomendacji.
- Bądź wyczulony na sensacyjne informacje, w szczególności zachęcające do natychmiastowego podjęcia jakiegoś działania. Weryfikuj informacje w kilku źródłach. **Upewnij się, że informacja jest prawdziwa przed podaniem jej dalej w mediach społecznościowych. Jeśli masz jakieś wątpliwości, wstrzymaj się.**
- Uważaj na wszelkie linki w wiadomościach mailowych i SMS-ach, zwłaszcza te sugerujące podjęcie jakiegoś działania, np. konieczność zmiany hasła, albo podejrzaną aktywność na koncie. Obserwowaliśmy w przeszłości tego typu celowane ataki na prywatne konta, gdzie celem było zdobycie informacji zawodowych.
- Upewnij się, że posiadasz kopię zapasową wszystkich ważnych dla siebie plików i potrafisz je przywrócić w przypadku takiej potrzeby.
- Śledź ostrzeżenia o nowych scenariuszach ataków na naszych mediach społecznościowych: Twitter, Facebook.
- Zgłaszaj każdą podejrzaną aktywność przez formularz na stronie incydent.cert.pl lub mailem na cert@cert.pl. Podejrzane SMS-y prześlij bezpośrednio na numer 799 448 084. Rekomendujemy zapisanie go w kontaktach.

Rekomendacje dla firm

Należy:

- Przetestować przywracanie infrastruktury z kopii zapasowych. **Kluczowe jest, żeby zostało to wykonane w praktyce na wybranych systemach, nie tylko proceduralnie.**
- Upewnić się, że posiadane **kopie zapasowe są odizolowane i nie ucierpią w przypadku ataku na resztę infrastruktury**.
- Upewnić się, że dokonywane są aktualizacje oprogramowania, **w szczególności dla systemów dostępnych z internetu**. Należy zacząć od podatności, które są na liście obecnie aktywnie wykorzystywanych w atakach.
- Upewnić się, że wszelki dostęp zdalny do zasobów firmowych wymaga uwierzytelniania dwuskładnikowego.
- Przejrzeć usługi w adresacji firmowej dostępne z internetu i ograniczyć je do niezbędnego minimum. Można w tym celu wykorzystać np. portal Shodan. W szczególności nie powinny być bezpośrednio dostępne usługi pozwalające na zdalny dostęp jak RDP czy VNC.

Źródło https://cert.pl/

- Aktualizować w sposób automatyczny sygnatury posiadanych systemów bezpieczeństwa typu AV, EDR, IDS, IPS, itd.
- Wdrożyć filtrowanie domen w sieci firmowej na bazie publikowanej przez nas listy ostrzeżeń. Dzięki temu w szybki sposób zablokowane zostaną zaobserwowane przez nas złośliwe domeny.
- Zapoznać się z przygotowanym przez CSIRT KNF poradnikiem dotyczącym obrony przed atakami DDoS i wdrożyć jego rekomendacje.
- Zapoznać się z poradnikiem omawiającym sposoby wzmocnienia ochrony przed ransomware i wdrożyć jego rekomendacje.
- Zapoznać się z materiałami dotyczącymi bezpieczeństwa haseł.
- Zapoznać się z artykułem dotyczącym mechanizmów weryfikacji nadawcy wiadomości i wdrożyć je dla domen wykorzystywanych do wysyłki poczty.
- W przypadku posiadania własnego zakresu adresów IP zalecamy dołączenie do platformy N6. Za jej pośrednictwem udostępniamy na bieżąco informacje o podatnościach i podejrzanej aktywności obserwowanej przez nas w podanym zakresie adresowym.
- Wyznaczyć osobę odpowiedzialną za koordynację działań w przypadku wystąpienia incydentu i przećwiczyć procedury reagowania.
- Uczulić pracowników na obserwację podejrzanej aktywności oraz poinformowanie o sposobie jej zgłaszania do wyznaczonej w firmie osoby.
- Zgłosić osobę kontaktową, nawet jeśli nie zobowiązuje do tego ustawa. Dzięki temu będziemy w stanie szybko skontaktować się z właściwą osobą w celu przesłania ostrzeżenia.
- Zgłaszać każdą podejrzaną aktywność do właściwego CSIRT-u, tj.:
    - CSIRT GOV — administracja rządowa i infrastruktura krytyczna,
    - CSIRT MON — instytucje wojskowe,
    - CSIRT NASK — wszystkie pozostałe.

Uwaga! Jeśli Twoja firma współpracuje z podmiotami na Ukrainie lub ma tam oddziały, dodatkowo:

- Sprawdź reguły dla dostępu sieciowego, ogranicz dozwolony ruch do minimum.
- Monitoruj ruch sieciowy, w szczególności na styku sieci z tymi firmami/oddziałami.
- Obejmij szczególnym monitoringiem hosty, na których jest zainstalowane oprogramowanie, które otrzymuje automatyczne aktualizacje od podmiotów na Ukrainie.
- Ostrzeż pracowników, aby byli szczególnie wyczuleni na informacje nakłaniające ich do podjęcia jakiegoś działania.

Źródło https://cert.pl/